Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application.

Listing of Claims:

1-31. (Cancelled)

32. (Currently Amended) A method for securely storing a key using a secure chip associated with a computer system, the method comprising:

creating a migratable keyblob, the migratable keyblob ~~containing~~ securely storing a key having been encrypted based at least in part on use of a first random number;

receiving user input creating a pass phrase to encrypt the first random number; and

encrypting the first random number using the pass phrase to prevent unauthorized usage of the first random number to decrypt and recover the key ~~contained~~ securely stored in the migratable keyblob,

wherein encrypting the first random number using the pass phrase comprises,

generating a pseudo-random number based on the pass phrase, the pseudo-random number having a same length as the first random number; and

XORing the first random number with the pseudo-random number to produce a string representing the encrypted first random number.

33. (Previously Presented) The method of claim 32, wherein generating a pseudo-random number based on the pass phrase includes:

hashing the pass phrase; and

applying a mask generation function to the hashed pass phrase.

34. (Previously Presented) The method of claim 32, further comprising storing the string representing the encrypted first random number.

35. (Previously Presented) The method of claim 34, wherein the storing the string representing the encrypted first random number includes storing the string on a hard disk associated with the computer system.

36. (Currently Amended) The method of claim 34, further comprising:

recovering the key securely stored in the migratable keyblob including,

receiving user input entering the pass phrase;

regenerating the pseudo-random number having a same length as the first random number based on the received pass phrase;

reproducing the first random number by XORing the regenerated pseudo-random number with the string representing the encrypted first random number; and

using the reproduced first random number to decrypt and recover the key ~~contained~~ securely stored in the migratable keyblob.

37. (Previously Presented) The method of claim 32, wherein the secure chip is a Trusted Platform Module (TPM) chip in accordance with Trusted Computing Platform Alliance (TCPA) protocols.

38. (Previously Presented) The method of claim 37, wherein the first random number is generated by the Trusted Platform Module (TPM) chip.

39. (Cancelled)

40. (Currently Amended) A computer readable medium with program instructions tangibly stored thereon for securely storing a key using a secure chip associated with a computer system, the computer readable medium comprising instructions for:

creating a migratable keyblob, the migratable keyblob ~~containing~~ securely storing a key having been encrypted based at least in part on use of a first random number;

receiving user input creating a pass phrase to encrypt the first random number; and

encrypting the first random number using the pass phrase to prevent unauthorized usage of the first random number to decrypt and recover the key ~~contained~~ securely stored in the migratable keyblob,

wherein the instructions for encrypting the first random number using the pass phrase comprise instructions for,

generating a pseudo-random number based on the pass phrase, the pseudo-random number having a same length as the first random number; and

XORing the first random number with the pseudo-random number to produce a string representing the encrypted first random number.

41. (Previously Presented) The computer readable medium of claim 40, wherein the instructions for generating a pseudo-random number based on the pass phrase include instructions for:

hashing the pass phrase; and

applying a mask generation function to the hashed pass phrase.

42. (Previously Presented) The computer readable medium of claim 40, further comprising instructions for storing the string representing the encrypted first random number.

43. (Previously Presented) The computer readable medium of claim 42, wherein the instructions for storing the string representing the encrypted first random number include instructions for storing the string on a hard disk associated with the computer system.

44. (Currently Amended) The computer readable medium of claim 42, further comprising instructions for:

recovering the key securely stored in the migratable keyblob including,

receiving user input entering the pass phrase;

regenerating the pseudo-random number having a same length as the first random number based on the received pass phrase;

reproducing the first random number by XORing the regenerated pseudo-random number with the string representing the encrypted first random number; and

using the reproduced first random number to decrypt and recover the key ~~contained~~ securely stored in the migratable keyblob.

45. (Previously Presented) The computer readable medium of claim 40, wherein the secure chip is a Trusted Platform Module (TPM) chip in accordance with Trusted Computing Platform Alliance (TCPA) protocols.

46. (Previously Presented) The computer readable medium of claim 45, wherein the first random number is generated by the Trusted Platform Module (TPM) chip.

47. (Currently Amended) A computer system comprising:

a secure chip to generate a first random number;

first circuitry coupled to the secure chip, the first circuitry operable to create a migratable keyblob, the migratable keyblob ~~contained~~ securely storing a key having been encrypted based at least in part on use of the first random number;

second circuitry couple to the first circuitry, the second circuitry to receive user input creating a pass phrase to encrypt the first random number; and

third circuitry coupled to the second circuitry, the third circuitry to encrypt the first random number using the pass phrase to prevent unauthorized usage of the first random number to decrypt and recover the key ~~contained~~ securely stored in the migratable keyblob, the third circuitry encrypting the random number using the pass phrase by,

generating a pseudo-random number based on the pass phrase, the pseudo-random number having a same length as the first random number; and

XORing the first random number with the pseudo-random number to produce a string representing the encrypted first random number.

48. (Previously Presented) The computer system of claim 47, further comprising a hard disk to store the encrypted first random number.

49. (Currently Amended) The computer system of claim 47, wherein the second circuitry is further operable to receive user input entering the pass phrase, and the computer system further comprises:

fourth circuitry coupled to the second circuitry, the fourth circuitry to decrypt the encrypted first random number and recover the first random number,

wherein the secure chip is operable to receive the migration keyblob and the recovered first random number to decrypt and recover the key ~~contained~~ securely stored in the migratable keyblob.

50. (Previously Presented) The computer system of claim 49, wherein the secure chip comprises a Trusted Platform Module (TPM) chip in accordance with Trusted Computing Platform Alliance (TCPA) protocols.